Description of Actual State Sensor Types for the Hardware Asset Management (HWAM) Capability

9 Jul 2014

1 Purpose

This document is intended to provide insight on the types of tools and technologies that can be utilized to support the collection of asset information required to perform the HWAM capability (as part of Continuous Diagnostics and Mitigation (CDM)). The 'Description of Generic Sensor Types for the Continuous Diagnostic and Mitigation (CDM) Collection System' document described the Actual State sensor types for CDM to include information about potential for operational impacts and general data accuracy issues associated with each particular sensor type.

The HWAM capability provides an organization visibility into the devices[1] connected to the network. Device data can be collected from many different points (i.e., sensors) on a network. These sensors collect data directly or indirectly from each device connected to the network. Sensors often have primary roles that do not necessarily include just collecting device data; however, during the process of performing its primary function (e.g., security or network management), the Actual State sensor collects detailed device data that can be extrapolated and used to support HWAM. Following are examples of how common protocols, devices, and functions can be employed as Actual State sensors to support the HWAM capability. Note, the collection capability and location of the sensor on the network relative to the device will determine the Actual State sensor type in which the protocol, device, or function is categorized.

[1] For CDM, the definition for device is: an IP-addressable asset on the network or a non-addressable component (e.g. removable media) able to interact with the organization's data and resources.

2 HWAM Actual State Sensor Types

2.1 Active Network Sensor

An Active Network Sensor actively probes the network or a device over the network.

An Active Network Sensor probes or queries devices on the network for current or existing asset information, to include associated removable media data. For HWAM, these sensors are configured to collect and report unique device and removable media identifying information. Examples of technologies or tools that act as Active Network Sensors for the HWAM capability include active network mappers, vulnerability scanners, and configuration checkers.

Vulnerability scanners or configuration checkers are better designed to support the Manage Vulnerabilities (VUL) and Manage Configurations Settings (CSM) respectively, however, each scanner collects device information for every device they scan on the network. That information could be used to identify authorized devices that were not present or “seen” in the operational environment during the last scan. Active network mappers scan IP ranges to discover devices communicating on the network. Depending on the network size, device scanners may take a considerable amount of time collecting results from each device residing on the network and not be able to collect the necessary data in an acceptable period of time. For example, larger enterprise networks with a large number of connected devices or removable media may take hours to collect results. It may not be feasible to scan frequently enough to detect all the device and removable media changes that could occur on such a large enterprise.

2.2 Passive Network Sensor

A Passive Network Sensor is designed to capture network traffic that passes across a monitored network link.

Passive Network Sensors only collect data that it is configured to identify—all other network traffic outside the configuration scope of the Passive Network Sensor will not be collected. Additionally, a Passive Network Sensor is unable to detect removable media associated with devices.

Networking protocols, packet analyzers and certain network devices are examples of passive network sensors that can support the HWAM capability. While these sensors are able to identify every device communicating over that network segment, the information collected is often a temporal identifier (i.e., IP address) and not easily translated into a unique device identifier that can be compared to the desired state inventory. Usually correlation with other Actual State sensor data is necessary to positively identify each device.

Network communications devices collect and store device data for all devices connected to the network. A Wireless Access Point (WAP) will collect and store a logical mapping of all media access control (MAC) addresses to IP addresses that connect to the WAP. Switches will also store device address data (i.e., MAC and IP addresses) for all devices connected (directly or indirectly) on each respective switch port. This device address data is often stored in content addressable memory (CAM) tables and is used to map MAC addresses to each port on the switch. Routers typically only store route information, i.e. (sub)network address, versus specific device IP addresses; however, in some circumstances device data could be ascertained if explicitly listed in the route table. For WAPs, switches, and routers, the device data for the networking device themselves could be acquired by parsing the configuration files of the networking device and extracting the specified management IP address.

Lastly, packet analyzers or sniffers act as passive network sensors by capturing data on all devices communicating on a network segment. At a minimum, a packet analyzer captures the device’s IP address but can also capture more content if configured to do so.

2.3 Asset Management Repository

An Asset Management Repository is a collection of data created and updated as part of a process or activity that manages that asset for an organization.

An Asset Management Repository aggregates managed device data collected by network management tools that are not deployed as part of CDM. Examples of Asset Management Repositories that can support the HWAM capability include Dynamic Host Configuration Protocol (DHCP) and Domain Name Service (DNS) servers, audit management systems, and certain networking protocols.

DHCP servers maintain a mapping of devices to IP addresses in the form of an IP address lease. IP leases bind an IP address to a client for a period of time (varies based on configuration) and stores this information on the DHCP server. DHCP servers are often consulted as a primary data source for device data due to the comprehensive repository of device IP address assignments.

Another location for device data is the DNS servers. Network address information is cataloged in DNS resource records (for both IPv4 and IPv6) providing a mapping between devices' hostnames and their statically assigned IP addresses. DNS name servers often don't inform if or when a device connects to the network; however, the resource records will provide a mapping of hostnames to IP addresses that supports accurate device identification.

Networking protocols that store device data for all network devices connected and communicating on the network can support the HWAM capability. Examples include the Address Resolution Protocol (ARP) and Simple Network Management Protocol (SNMP). ARP records the device's MAC address to IP address mapping for each device communicating on the subnet. This link layer to network layer coupling is buffered in ARP tables on all devices sharing a common subnet. If installed and configured for network management, SNMP can provide detailed information about managed devices. Device information acquired by SNMP is collected from managed devices and often stored in a centralized network management repository.

Lastly, audit management systems that collect device audit data and store it for further analysis and reporting can also support the HWAM capability as an Actual State sensor. These sensors provide the ability to gather identifying information about a device and any removable media inserted into that device. The frequency of the audit will determine how up-to-date the device and removable media data is that's stored in the repository.

2.4 Network Event Sensor

A Network Event Sensor is designed to detect and report events of interest to a defined location in a timely manner.

Network event sensors provide situational awareness of unauthorized events that take place on the network. These sensors perform this by monitoring and alerting on predefined audit security and compliance relevant information received from in-scope devices. Managed devices on the network forward audit log data via specified management protocols to a Network Event Sensor. What events to report and when to report is defined by the parameters of the security policy that are in-turn applied to each in-scope device. Once the Network Event Sensor receives events, the events can be analyzed through real-time data correlation and analysis of historical trends to track security-related configuration settings.

Examples of common technologies that can be employed as Actual State sensors supporting the HWAM capability include security information and event management (SIEM) tools, intrusion detection or prevention systems (IDS/IPS), firewalls, and proxy devices.

Security information and event management (SIEM) tools aggregate logs from various sensors providing the ability to consolidate and correlate device data. This aggregation of data from various sources leads to greater device data accuracy. SIEMs collect, analyze, and transform large amounts of data into actionable intelligence for network management and security. Device data can be extrapolated from this large data set and used to support the HWAM capability.

Security devices such as IDS/IPS, firewalls, and proxies record device data by detecting and logging devices communicating on the network they are positioned and configured to monitor. Their primary function is network security but in the process of monitoring for suspicious or malicious activity they log and report device address information that can be collected to correlate device activity on the network.

2.5 Endpoint-Based Agent

An Endpoint-Based Sensor is a software client installed on, or natively embedded within, the operating system of a device.

Endpoint-Based Agents collect and report device and associated removable media data, directly from the device. This method of collecting HWAM data is the most direct and accurate; however, it requires an installed agent for every managed device resulting in an increase in management overhead. Examples of Endpoint-Based Agents include host-based intrusion detection systems (HIDS), built-in functionality/features of the operating system (OS), or embedded hardware audit agents.

An example of an Endpoint-Based Agent collecting and reporting device data includes a Windows OS reading an IP address directly from the interface configuration. Another example includes a script or software package installed as a resident Endpoint-Based Agent that retrieves stored (i.e. logged) universal serial bus (USB) serial numbers from a device. USB serial numbers are often recorded in the Windows USB storage port driver (USBSTOR) registry key when USBs are connected to a device. Audit agents that are capable of "pushing" audit event information, such as when a network address is assigned to an interface, is another example. HWAM data elements can be collected but how often it is reported determines the timeliness of the data.